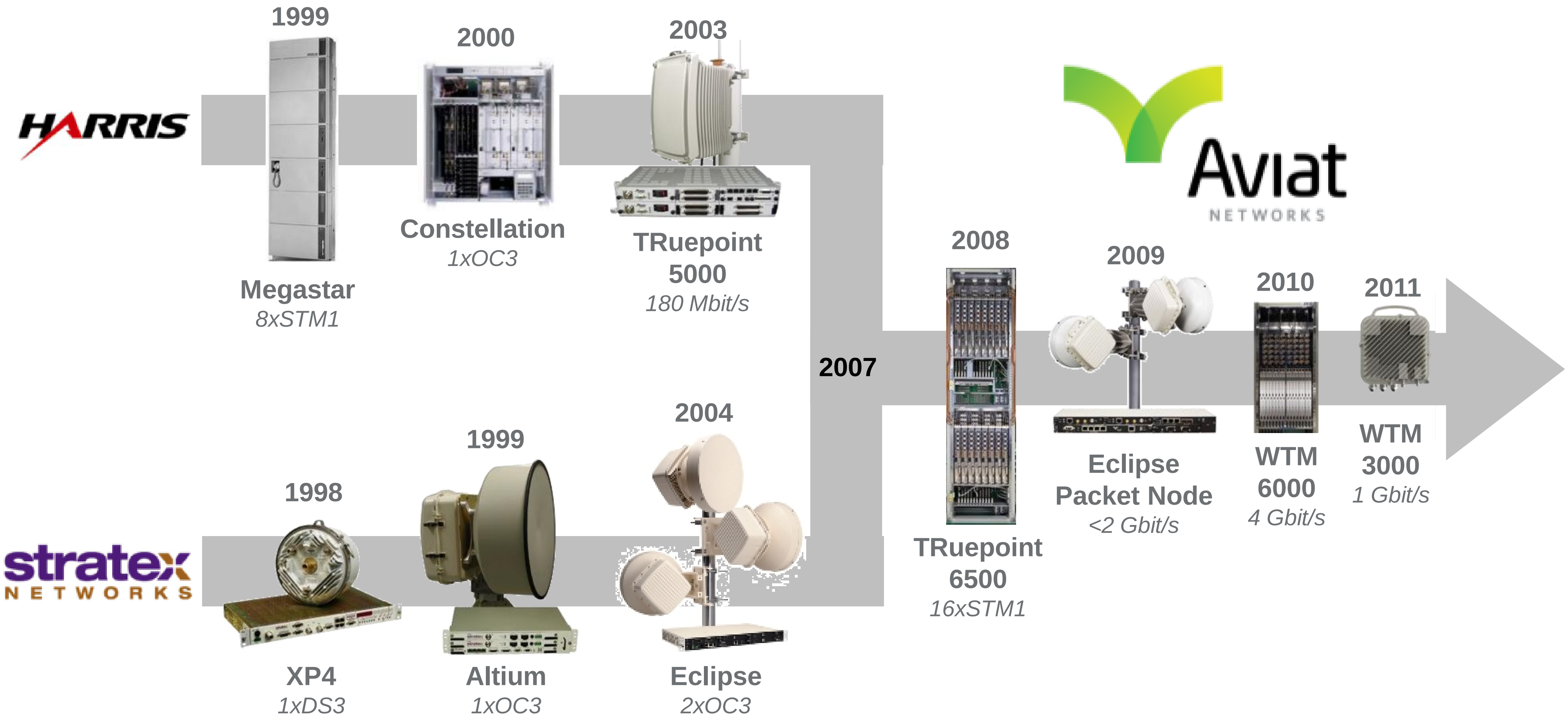
Aviat
NETWORKS

IP/ETHERNET REDUNDANCY AND PROTECTION FOR MICROWAVE SYSTEMS

ROBIN SIMS, DIRECTOR U.S. GOVERNMENT INITIATIVES
GARY CROKE, PRODUCT MARKETING

DESIGNED•BUILT
SUPPORTED•IN THE USA

Aviat Networks Product Evolution



HARRIS

1999
Megastar
8xSTM1

2000
Constellation
1xOC3

2003
TRuepoint 5000
180 Mbit/s

stratex NETWORKS

1998
XP4
1xDS3

1999
Altium
1xOC3

2004
Eclipse
2xOC3

2007

Aviat NETWORKS

2008
TRuepoint 6500
16xSTM1

2009
Eclipse Packet Node
<2 Gbit/s

2010
WTM 6000
4 Gbit/s

2011
WTM 3000
1 Gbit/s

Our North American Utility Customers

PSEG

Progress Energy

AEP AMERICAN ELECTRIC POWER

ComEd
An Exelon Company

CHUGACH
POWERING ALASKA'S FUTURE

Nevada Power.

PACIFIC POWER

Ameren

AEP INDIANA MICHIGAN POWER
A unit of American Electric Power

NVEnergy.

BC hydro

nationalgrid

DTE Energy

hydro one

ATCO Electric

Williams.

Sempra Energy

PG&E

SDGE

Hawaiian Electric Company, Inc.
Giving you the power

South Florida Water Management District

ATCO Gas

elpaso

NorthWestern Energy

BGE

e·on U.S.

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

LA DWP Los Angeles Department of Water & Power

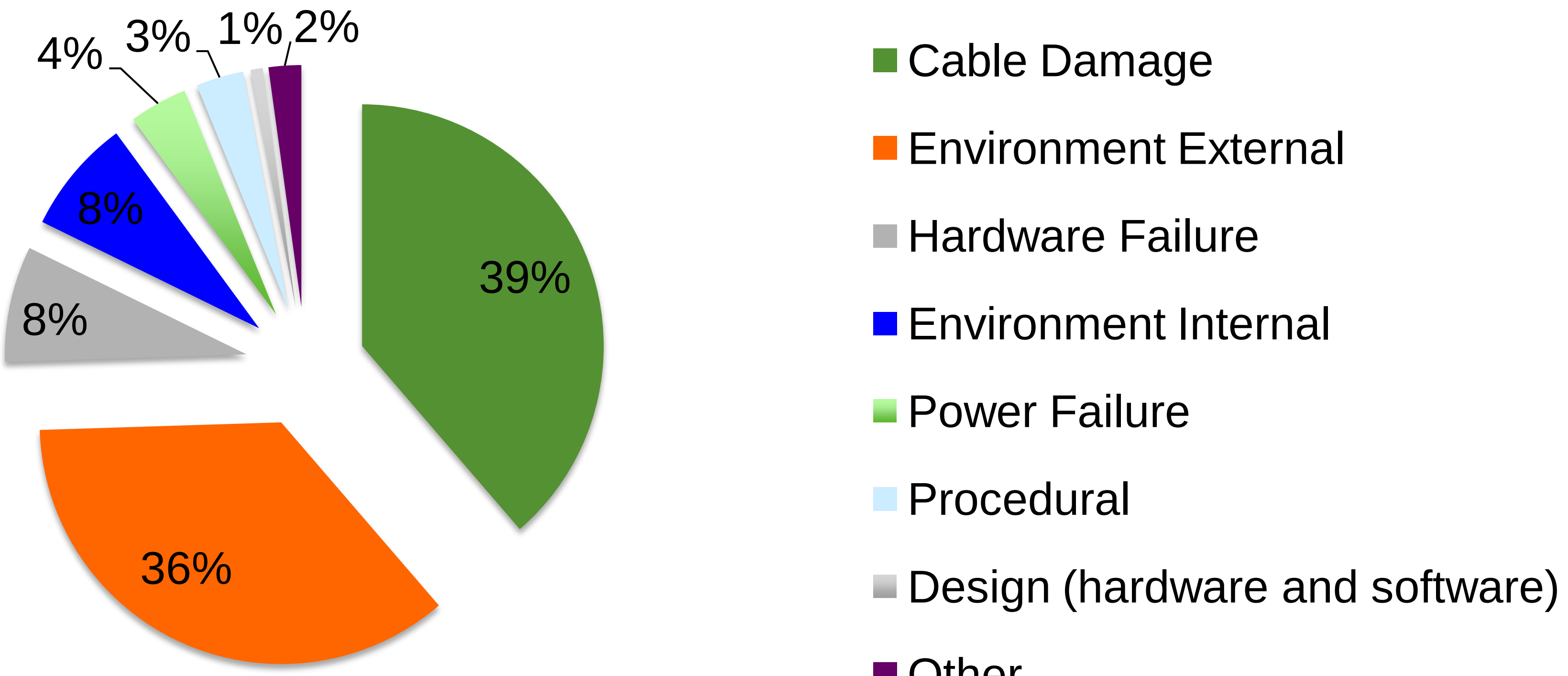
Why Are We Here?

	TDM	IP
Attributes	Fixed bandwidth. End-End for duration of call/circuit	Variable bandwidth. Packet by packet routing. No end-end awareness
Predictable	**Yes** Circuit switched connections	**No** "Hop by hop" routing – no end-end knowledge of packet path
Secure	**Yes** Requires physical port access – no "addressability"	**Not inherently** Ubiquitous addressing, open communication. Secure protocols / tools available
Resilient	**Yes** Proven 50ms failure recovery schemes	**No** Routing protocol "convergence" in multiple seconds
Cost Effective	**No** High cost per bit transmitted	**Yes** Economies of scale drives costs down
Scalable	**No** Dedicated connections mean poor use of b/w. No statistical multiplexing	**Yes** Only send data when required. Statistical multiplexing
New Services	**No** Must adapt to TDM frame	**Yes** New applications built to run on IP

IP makes reliability *more important* and *more complicated*

Most Common Sources of Failures

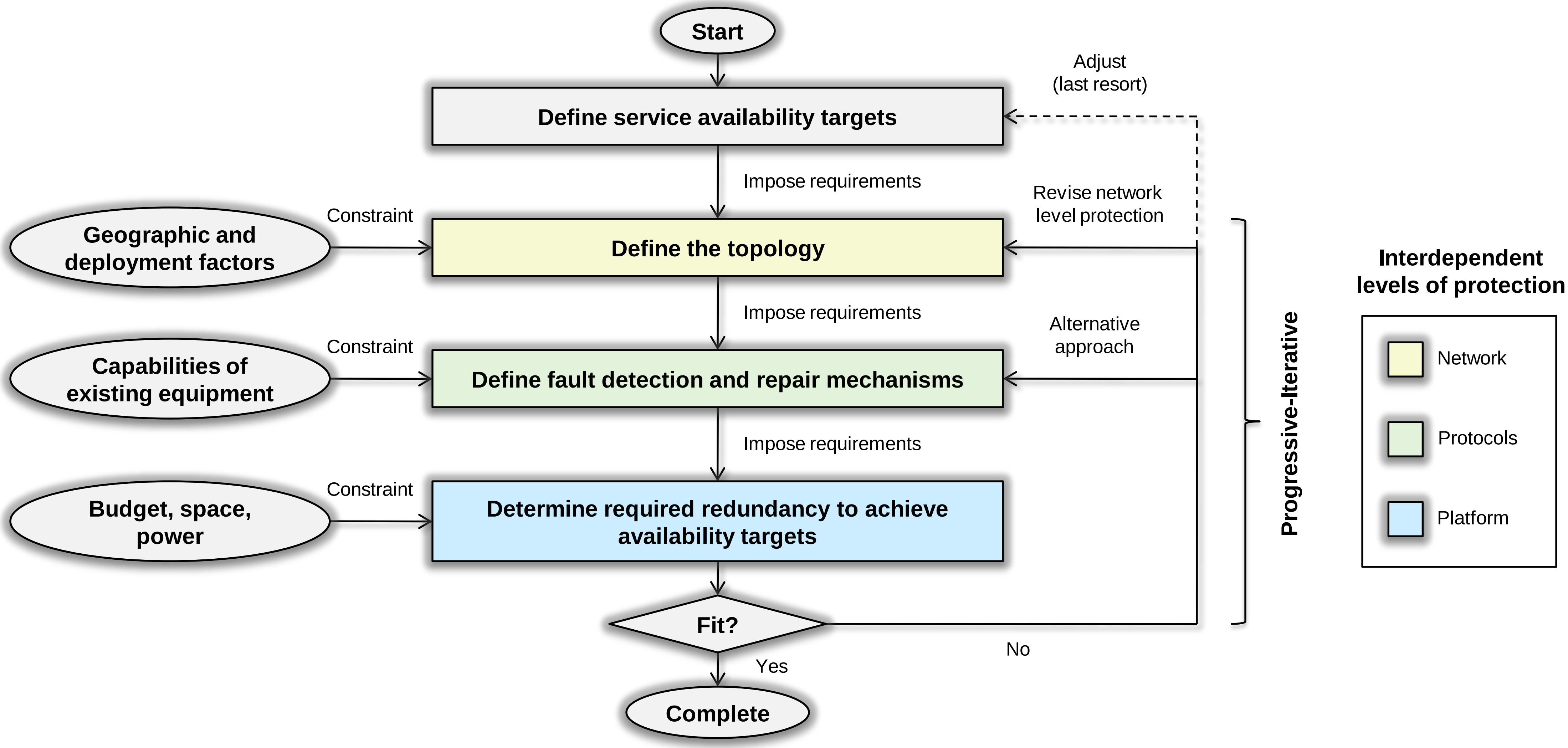
Root Causes of Network Failures



Source: ATIS, 2009

Natural events and “man-made” conditions most common

Protection Levels and Discovery Process



Start
Adjust
(last resort)
Define service availability targets
Impose requirements
Revise network level protection
Geographic and deployment factors
Constraint
Define the topology
Impose requirements
Alternative approach
Capabilities of existing equipment
Constraint
Define fault detection and repair mechanisms
Impose requirements
Budget, space, power
Constraint
Determine required redundancy to achieve availability targets
Fit?
No
Yes
Complete
Progressive-Iterative
Interdependent levels of protection
Network
Protocols
Platform

Employ top-down approach to break problem statement into smaller pieces

Reliability is Big Topic: Focus on 4 Features Today

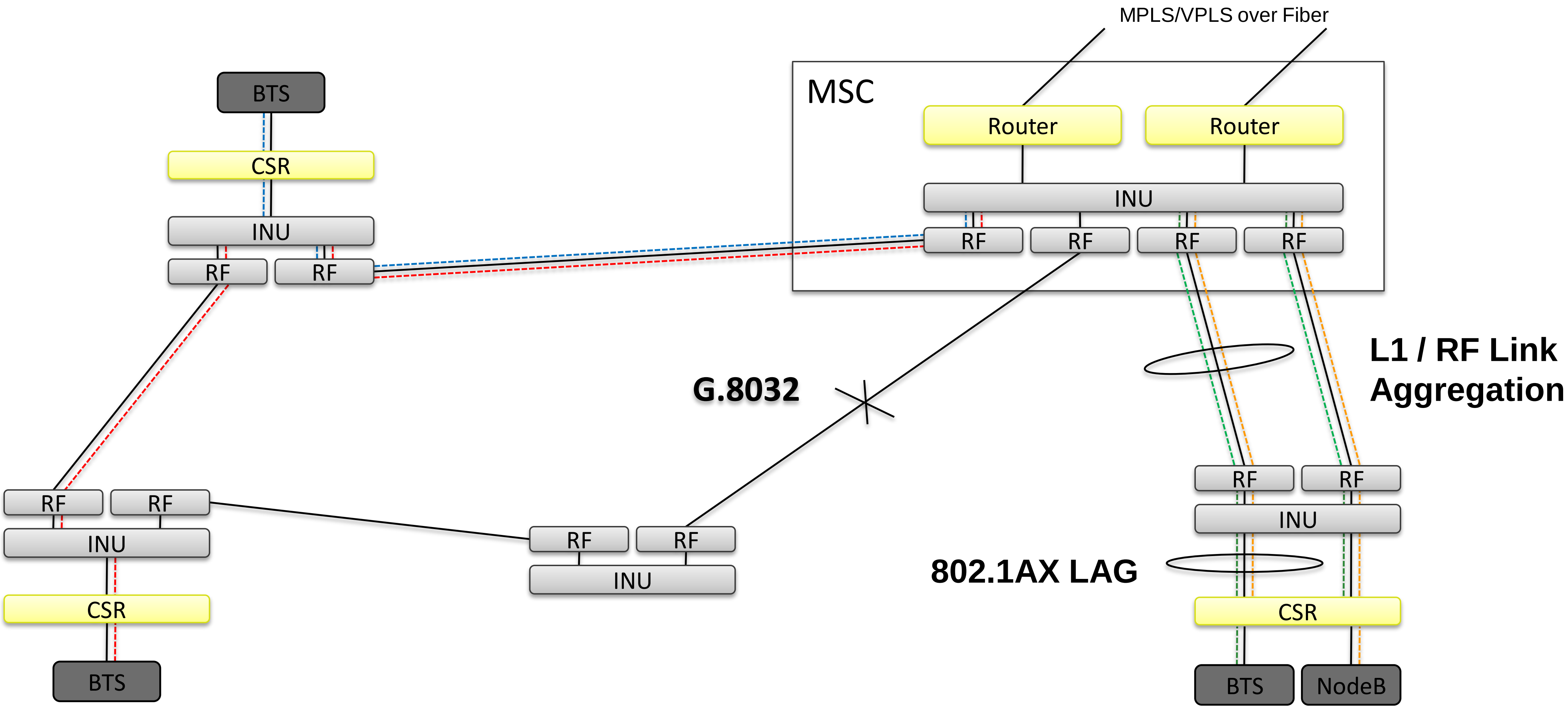
G.8032

N+0
(with Link Aggregation)

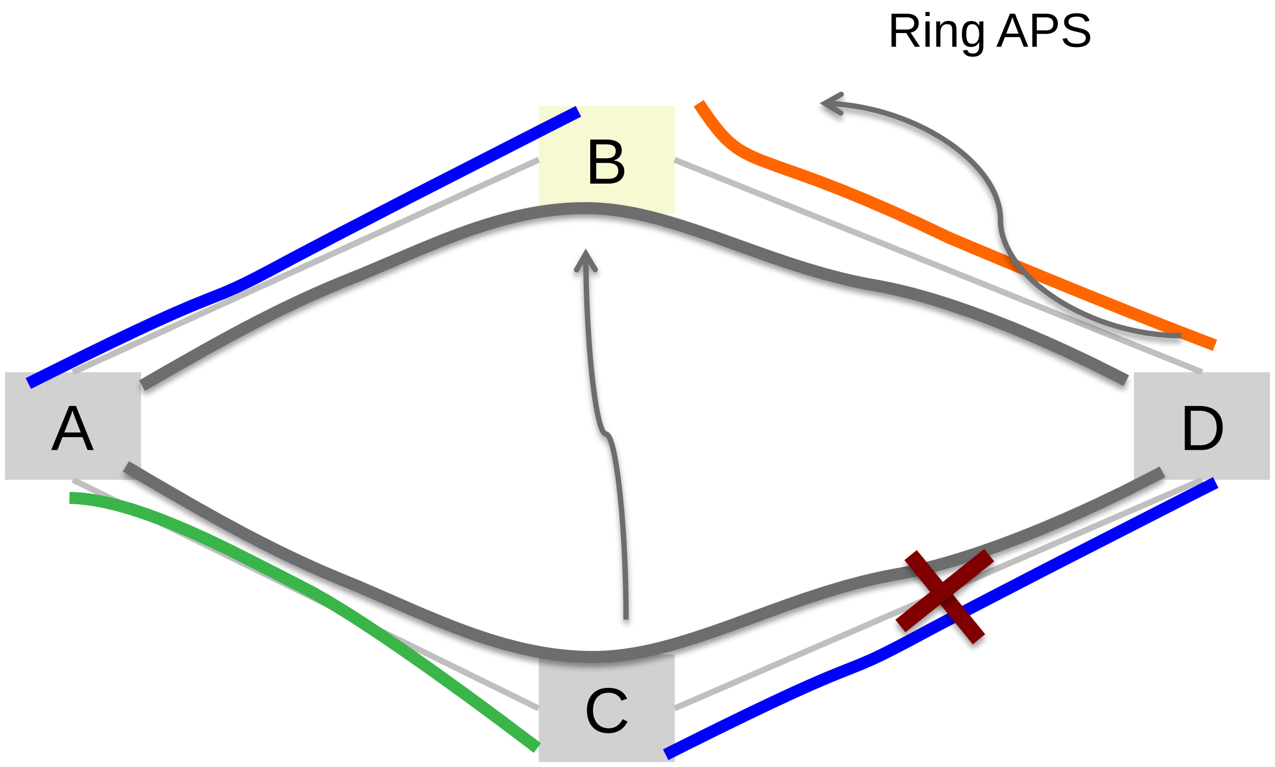
Strong Security
(update)

ACM
(update)

Failure Scenarios



G.8032: How it works…



All within 50ms

1. RPL owner (B) blocks one link from topology (to prevent loops). Nodes use topology to create forwarding entries

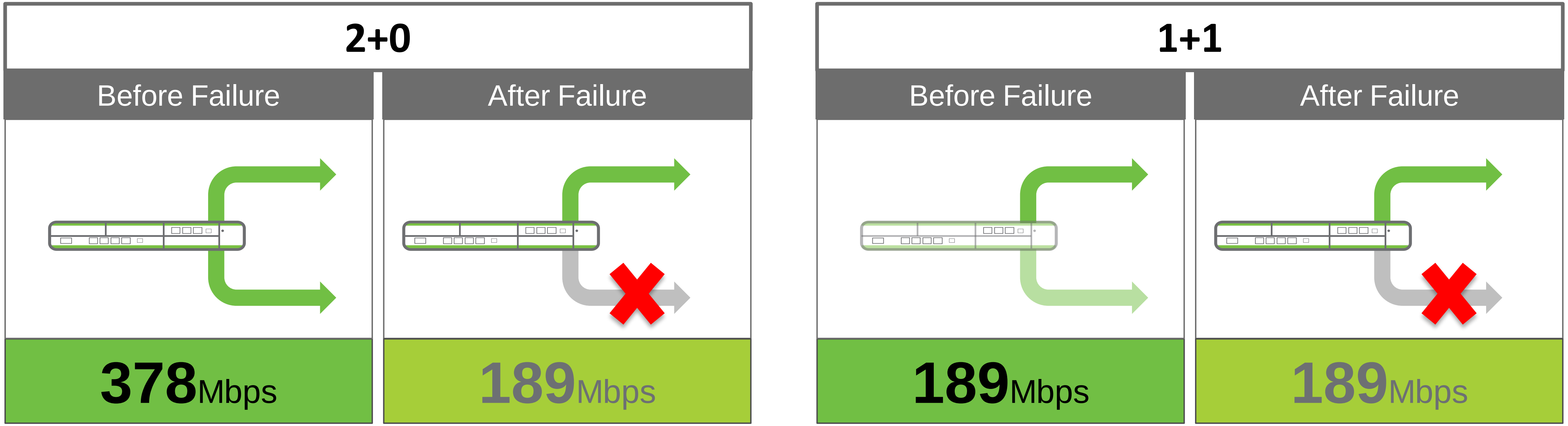
2. Failure occurs and is detected by physical layer monitoring and Y.1731 CCM messages every 3.3ms

3. Nodes signal ring APS request to RPL owner

4. RPL owner unblocks link and notifies other nodes. All nodes perform forwarding DB flush and fwd packets based on new ring topology with link unblocked.

5. Reversion configurable

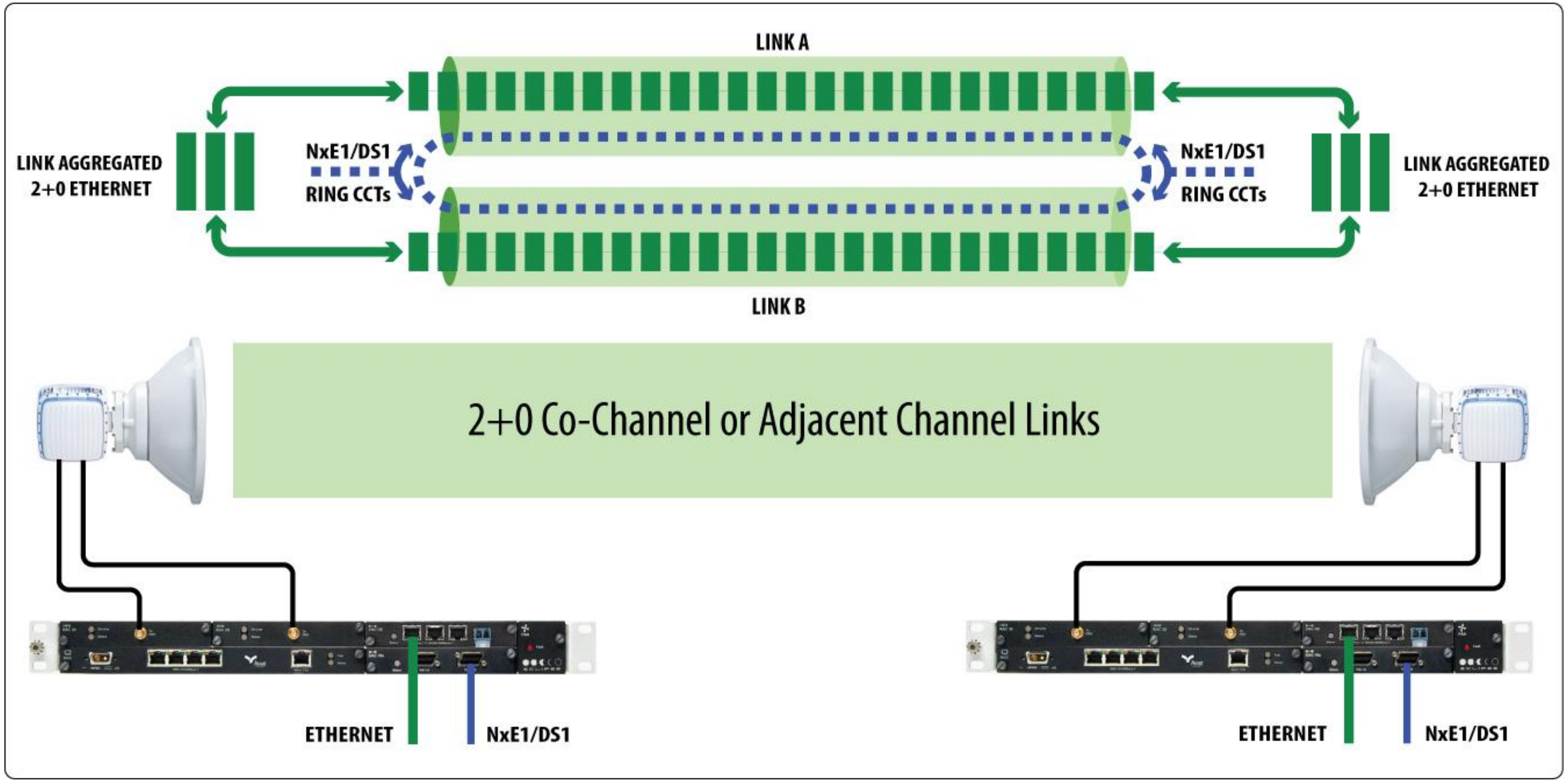
N+0 is One of The Best Ways to Grow Capacity



2+0		1+1	
Before Failure	After Failure	Before Failure	After Failure
378 Mbps	**189**Mbps	**189**Mbps	**189**Mbps

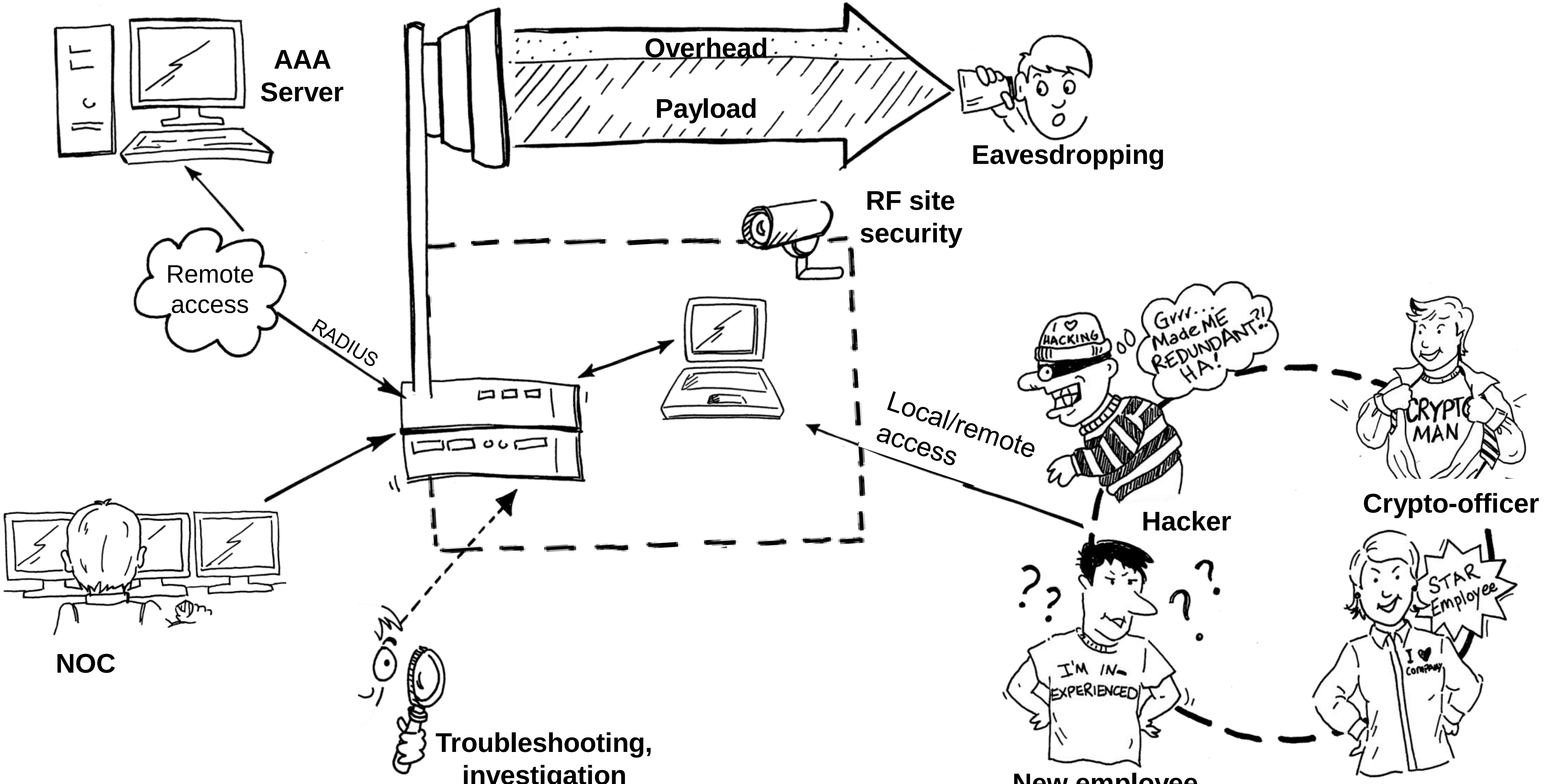
But You Need QoS…

And Ethernet + TDM (2+0 Ethernet with 1+1 TDM)


LINK A
LINK AGGREGATED 2+0 ETHERNET
NxE1/DS1
RING CCTs
NxE1/DS1
RING CCTs
LINK AGGREGATED 2+0 ETHERNET
LINK B
2+0 Co-Channel or Adjacent Channel Links
ETHERNET
NxE1/DS1
ETHERNET
NxE1/DS1

Possible ONLY with Hybrid Radios

Microwave Security is More Important with IP



AAA Server

Overhead

Payload

Eavesdropping

RF site security

Remote access

RADIUS

Local/remote access

Hacker

Crypto-officer

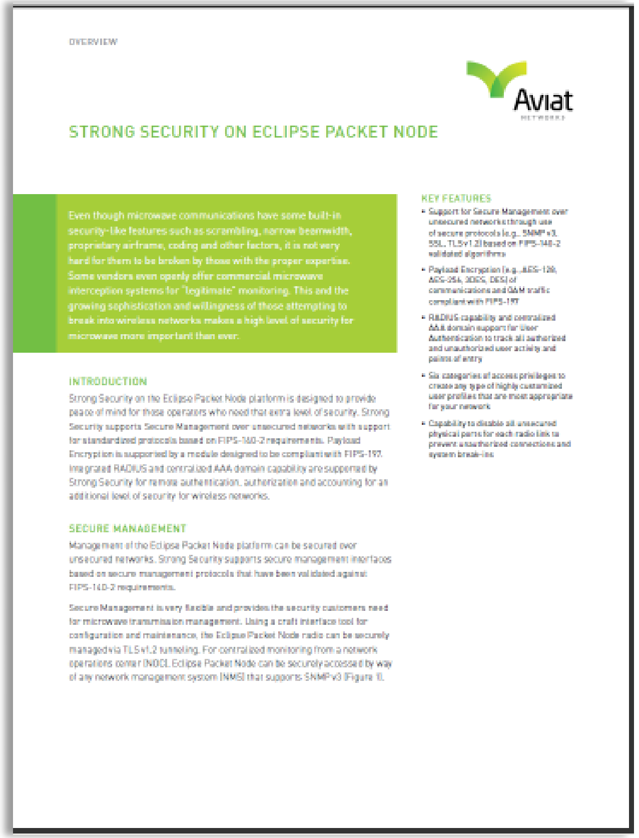
NOC

Troubleshooting, investigation

New employee or contractor

Related Collateral

Strong Security Overview



OVERVIEW

STRONG SECURITY ON ECLIPSE PACKET NODE

Even though microwave communications have some built-in security-like features such as scrambling, narrow beamwidth, proprietary airframe, coding and other factors, it is not very hard for them to be broken by those with the proper expertise. Some vendors even openly offer commercial microwave interception systems for "legitimate" monitoring. This and the growing sophistication and willingness of those attempting to break into wireless networks makes a high level of security for microwave more important than ever.

INTRODUCTION

Strong Security on the Eclipse Packet Node platform is designed to provide peace of mind for those operators who need that extra level of security. Strong Security supports Secure Management over unsecured networks with support for standardized protocols based on FIPS-140-2 requirements. Payload Encryption is supported by a module designed to be compliant with FIPS-197. Integrated RADIUS and centralized AAA domain capability are supported by Strong Security for remote authentication, authorization and accounting for an additional level of security for wireless networks.

SECURE MANAGEMENT

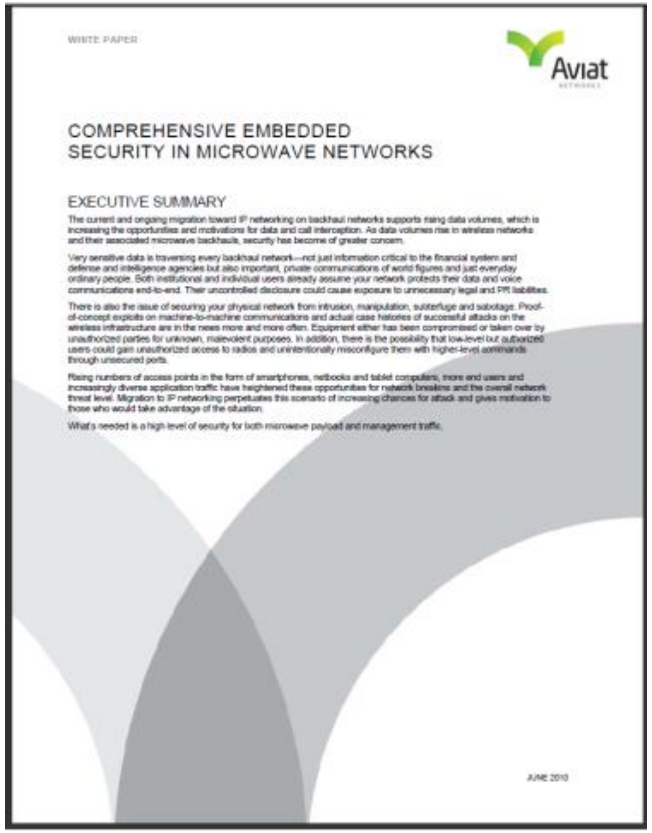
Management of the Eclipse Packet Node platform can be secured over unsecured networks. Strong Security supports secure management interfaces based on secure management protocols that have been validated against FIPS-140-2 requirements.

Secure Management is very flexible and provides the security customers need for microwave transmission management. Using a craft interface tool for configuration and maintenance, the Eclipse Packet Node radio can be securely managed via TLS v1.2 tunneling. For centralized monitoring from a network operations center (NOC), Eclipse Packet Node can be securely accessed by way of any network management system (NMS) that supports SNMP v3 (Figure 1).

KEY FEATURES

- Support for Secure Management over unsecured networks through use of secure protocols (e.g., SNMP v3, SSL, TLS v1.2) based on FIPS-140-2 validated algorithms
- Payload Encryption (e.g., AES-128, AES-256, 3DES, DES) of communications and O&M traffic compliant with FIPS-197
- RADIUS capability and centralized AAA domain support for User Authentication to track all authorized and unauthorized user activity and points of entry
- Six categories of access privileges to create any type of highly customized user profiles that are most appropriate for your network
- Capability to disable all unsecured physical ports for each radio link to prevent unauthorized connections and system break-ins

Strong Security White Paper



WHITE PAPER

COMPREHENSIVE EMBEDDED SECURITY IN MICROWAVE NETWORKS

EXECUTIVE SUMMARY

The current and ongoing migration toward IP networking on backhaul networks supports rising data volumes, which is increasing the opportunities and motivations for data and call interception. As data volumes rise in wireless networks and their associated microwave backhauls, security has become of greater concern.

Very sensitive data is traversing every backhaul network—not just information critical to the financial system and defense and intelligence agencies but also important, private communications of world figures and just everyday ordinary people. Both institutional and individual users already assume your network protects their data and voice communications end-to-end. Their uncontrolled disclosure could cause exposure to unnecessary legal and PR liabilities.

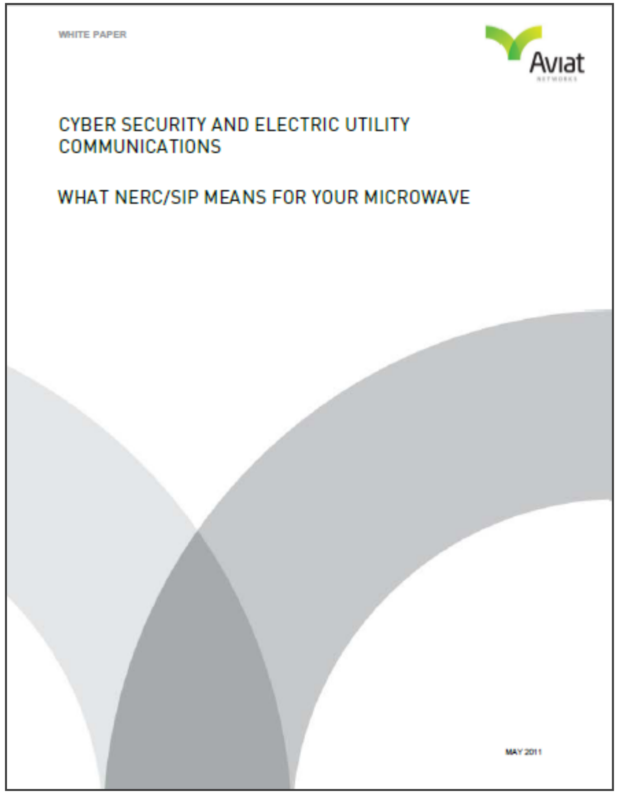
There is also the issue of securing your physical network from intrusion, manipulation, subterfuge and sabotage. Proof-of-concept exploits on machine-to-machine communications and actual case histories of successful attacks on the wireless infrastructure are in the news more and more often. Equipment either has been compromised or taken over by unauthorized parties for unknown, malevolent purposes. In addition, there is the possibility that low-level but authorized users could gain unauthorized access to radios and unintentionally misconfigure them with higher-level commands through unsecured ports.

Rising numbers of access points in the form of smartphones, netbooks and tablet computers, more end users and increasingly diverse application traffic have heightened these opportunities for network breakins and the overall network threat level. Migration to IP networking perpetuates this scenario of increasing chances for attack and gives motivation to those who would take advantage of the situation.

What's needed is a high level of security for both microwave payload and management traffic.

JUNE 2010

CYBER SECURITY AND ELECTRIC UTILITY COMMUNICATIONS



WHITE PAPER

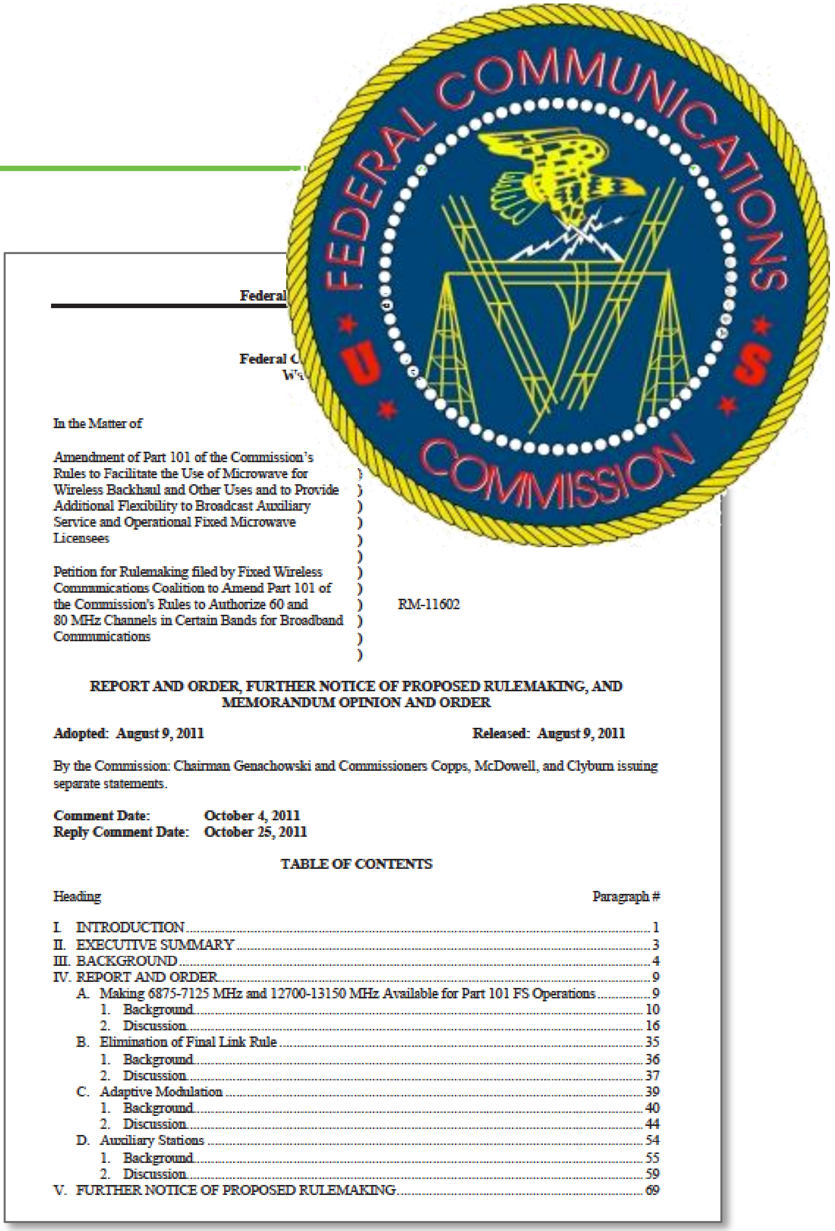
CYBER SECURITY AND ELECTRIC UTILITY COMMUNICATIONS

WHAT NERC/SIP MEANS FOR YOUR MICROWAVE

MAY 2011

New FCC Changes on ACM

- Previously, all links deployed 6, 10, 11GHz bands must meet minimum bits/Hz at all times (Part 101.141):
  - Eg: 30MHz channel - 89.4 Mbps @11GHz, 134.1Mbps @6GHz
- New FCC Rulemaking (October 2011):
  - Operation below minimum payload capacity is now permitted
  - Must operate higher than minimum payload capacity for 99.95% of the time (262.8 minutes allowed below minimum bandwidth)
  - No logging of ACM usage or equipment timers
- FCC Licensing:
  - Data/bit rate, emission designator, transmit power that will be used on the path
  - Each modulation step must be listed on the license application
  - No extra fees from Comsearch for link licensing when ACM is available


FEDERAL COMMUNICATIONS COMMISSION
U
S

Federal

Federal C
W

In the Matter of

Amendment of Part 101 of the Commission's)
Rules to Facilitate the Use of Microwave for)
Wireless Backhaul and Other Uses and to Provide)
Additional Flexibility to Broadcast Auxiliary)
Service and Operational Fixed Microwave)
Licensees)
)
Petition for Rulemaking filed by Fixed Wireless)
Communications Coalition to Amend Part 101 of)
the Commission's Rules to Authorize 60 and) RM-11602
80 MHz Channels in Certain Bands for Broadband)
Communications)
)

REPORT AND ORDER, FURTHER NOTICE OF PROPOSED RULEMAKING, AND MEMORANDUM OPINION AND ORDER

Adopted: August 9, 2011 **Released: August 9, 2011**

By the Commission: Chairman Genachowski and Commissioners Copps, McDowell, and Clyburn issuing separate statements.

Comment Date: October 4, 2011
Reply Comment Date: October 25, 2011

TABLE OF CONTENTS

Heading Paragraph #

Platform Reliability: High Availability Microwave Checklist

What should I look for?	How can I qualify it?
No single point of failure	Redundant radios, Ethernet modules, power supplies, fans, traffic buses
Multiple radio link protection options	Support for HSB, N+0, ACM, space diversity, and media diversity
Facilitates fast physical access for MTTR reduction	All-indoor radio
Permits in-service hardware and cabling maintenance	Modules swappable without traffic hits, stacking support for seamless Ethernet capacity upgrade, dual-feed support
Minimal traffic impact during software upgrades	Ability to schedule software upgrades based on ToD and intelligently sequence upgrade process for redundant systems
≤ 50 msec traffic impact for all common failure scenarios	Carrier Ethernet network protocol support (ring protection, aggregation, detection mechanisms) and internal health monitoring of all modules
Ability to defend from human error and unauthorized access	Storm protection and secure management with robust user authentication
Tools for quick fault identification and isolation	Integrated Ethernet OAM MIP and MEP with CFM (continuity check, loopback, link trace) and proactive frame loss measurements support
Management process	Automated discovery of topology and ACM changes, correlation with fault and performance data, proactive scheduled network health reporting

A Changing Environment…

Can be managed with smart microwave decisions

Upcoming Aviat Educational Events

Live Video Streaming Webinars

Topic	Date
Ethernet Redundancy	Replay Available
Microwave Capacity Analysis	Replay Available
★ Microwave Architectures	May 2012

Advanced Microwave Technology Seminar

★ April 24/25, 2012 Dallas TX	**Day 1** Network migration - TDM to IP Carrier Ethernet Transport & MPLS LTE requirements on backhaul Ethernet radio capacity analysis Network Timing and Synchronization **Day 2** ACM Microwave Strong Security Microwave antenna tech update Outsourced network operations

Email: **marketing@aviatnet.com**

Aviat
NETWORKS

AVIATNETWORKS.COM

DESIGNED•BUILT
SUPPORTED•IN THE USA

Why Are We Here?

How to bring “tank-like” reliability to IP microwave networks

why IP Reliability?

	TDM	IP
Predictable	yes	no
Secure	yes	not inherently
Resilient	yes	no
Cost Effective	no	yes
Scalable	no	yes
New Services	no	yes

FOCUS